Deutscher Bundestag **Drucksache 17/6619**

17. Wahlperiode 15. 07. 2011

Kleine Anfrage

der Abgeordneten Sylvia Kotting-Uhl, Dr. Konstantin von Notz, Harald Ebner, Hans-Josef Fell, Bettina Herlitzius, Bärbel Höhn, Oliver Krischer, Stephan Kühn, Undine Kurth (Quedlinburg), Ingrid Nestle, Dorothea Steiner, Daniela Wagner, Dr. Valerie Wilms und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Sicherheitsrelevanz hochentwickelter Schad-Software wie Stuxnet für deutsche Atomkraftwerke und industrielle Prozesssteuerung

Nachdem im Herbst letzten Jahres bekannt wurde, dass eine hochentwickelte Schad-Software (sog. Malware) namens Stuxnet irreparable Schäden an Komponenten iranischer Atomanlagen verursacht hatte, kam auch hierzulande schnell die Frage auf, inwiefern deutsche Atomkraftwerke (AKW) durch Stuxnet oder andere vergleichbar hochentwickelte Malware bedroht sein könnten. Medienberichte der letzten Monate deuten kontinuierlich darauf hin, dass ein von Malware wie Stuxnet ausgehendes Risiko für deutsche AKW vorhanden ist, dass über den Einzelfall hinaus vor allem spezialisierte Programme zur industriellen Prozesssteuerung betrifft (vgl. beispielsweise „Der digitale Erstschlag ist erfolgt“ in Frankfurter Allgemeine Zeitung vom 22. September 2010, „Landkarte des Schreckens“ in DER SPIEGEL 12/2011 vom 21. März 2011, „Deutsche Energieversorger anfällig für Computerwurm Stuxnet“ in DER SPIEGEL 16/2011 vom 18. April 2011 und „Siemens bestätigt Schwachstellen in Industrie-Software“, SPIEGEL ONLINE vom 19. Mai 2011).

Die Stellungnahmen deutscher Atomaufsichtsbehörden beschränken sich im Wesentlichen darauf, dass bisher noch kein Befall deutscher AKW festgestellt wurde. Zur Anfälligkeit der Anlagen und zur Wirksamkeit möglicher Gegenmaßnahmen gibt es bislang noch keine belastbaren Aussagen. Fest steht lediglich, dass Stuxnet als Teil des Schädigungsmechanismus Steuerungsanlagen der Firma Siemens AG befällt, die auch in deutschen Atomkraftwerken eingesetzt werden.

Das Programm nutzte nach heutigem Kenntnisstand vier bis dato nicht identifizierte Sicherheitslücken (Zero-Day-Exploits) des Betriebssystems Windows und manipulierte vor allem Anlagen des deutschen Herstellers Siemens AG, wobei u. a. die Steuersoftware WinCC (Windows Control Center) und das Prozessleitsystem SIMATIC PCS 7 beeinträchtigt werden. WinCC dient der Visualisierung von in Raffinerien, Kraftwerken und Fabriken ablaufenden Prozessen und wird meist in deren Leitstand eingesetzt. PCS 7 steuert und überwacht automatisierte Betriebsabläufe. Die Schad-Software wurde als Trojaner so auf den befallenen Anlagen platziert, dass sie möglichst lange unentdeckt bleiben sollte.

Um die sicherheitstechnische Bedeutung von Malware wie Stuxnet bewerten zu können, müssten die Landesatomaufsichtsbehörden und das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) zumindest wissen, welche potenziell befallbaren Siemens-Steuerungsanlagen in welchen Be-

reichen welcher deutscher Atomkraftwerke und anderer kritischer Infrastrukturen betrieben werden. Dies war ein halbes Jahr, nachdem die Frage von der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH in Form einer Weiterleitungsnachricht am 30. September 2010 aufgegriffen wurde, aber nicht der Fall, wie aus einem Brief vom Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Dr. Norbert Röttgen, an die Bundestagsabgeordnete Sylvia Kotting-Uhl vom 31. März 2011 hervorgeht. Demnach scheint bislang auch nicht klar, wie ein Befall von Malware wie Stuxnet der in den AKW eingesetzten Rechnern über Intranetverbindungen, Internetverbindungen, USB-Anschlüsse, DVD- und CD-Laufwerke etc. wirksam unterbunden werden kann.

Ebenfalls wurde bislang noch nicht durch spezifische Untersuchungen bestätigt, dass ein Stuxnet-Befall und andere mögliche Malware-Infektionen tatsächlich keine Auswirkungen auf das Reaktorschutzkonzept haben kann. Die GRS mbH stellt diese These in ihrer Weiterleitungsnachricht bereits auf, räumt zugleich aber ein, den tatsächlichen Umfang der Sicherheitsbedeutung von Stuxnet noch nicht abschätzen zu können.

Dabei stellt sich insbesondere die Frage, ob Malware wie Stuxnet den Reaktorbetrieb unbemerkt aus den definierten Zuständen herausführen kann, die Grundlage der Störfallbeherrschung sind. Anders ausgedrückt stellt sich die Frage, ob Malware wie Stuxnet den Zustand oder das Verhalten einzelner Kraftwerkskomponenten verändern kann und zugleich diejenigen Informationen über den Zustand und das Verhalten der befallenen Komponenten, die an Anzeigen und Kontrollsysteme übermittelt werden, verfälschen kann. Wäre dies der Fall, könnte nicht ausgeschlossen werden, dass die automatische Störfallbeherrschung und die Handlungen des Personals zur Störfallbeherrschung völlig andere Wirkungen hervorrufen als erwartet und gewünscht.

Es ist nach Angaben von IT-Sicherheitsexperten davon auszugehen, dass es sich bei dem nun entdeckten Schadprogramm mit hoher Wahrscheinlichkeit nicht um das erste Programm dieser Art handelt, Stuxnet vielmehr aufgrund eines anzunehmenden Programmierfehlers eher zufällig entdeckt worden sei und davon ausgegangen werden muss, dass sich in Zukunft ähnliche Angriffe auf Industrieanlagen wiederholen. So wird der deutsche IT-Sicherheitsexperte Prof. Dr. Thorsten Holz mit den Worten zitiert: „Ich halte diesen Angriff nicht für den ersten dieser Art und bei allem Aufwand auch nicht für einmalig. Ich gehe davon aus […], dass solche Angriffe häufiger vorkommen, dass die erfolgreichen aber nicht öffentlich bekannt werden.“ (SPIEGEL ONLINE vom 22. September 2010)

Wir fragen die Bundesregierung:

1. Warum war innerhalb eines halben Jahres nicht zu klären, welche Steuerungsanlagen in welchen AKW in welchen Bereichen eingesetzt werden (vgl. erste Empfehlung der GRS-Weiterleitungsnachricht vom 30. September 2010 und Brief von Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Dr. Norbert Röttgen, an die Bundestagsabgeordnete Sylvia Kotting-Uhl vom 31. März 2011)?

2. Ist mittlerweile klar, in welchen AKW in welchen Bereichen die Siemens-Software und Steuerungsanlagen, auf die Stuxnet abzielt, eingesetzt werden (ggf. bitte für die AKW, zu denen die Informationen mittlerweile vorliegen, anlagenscharfe tabellarische Übersicht mit Anzahl, Typ, Anlagenbereich, Einsatzzweck etc.)?

   Falls nein, weshalb nicht, bis wann soll dies endgültig für alle AKW geklärt sein?

3. Falls bislang immer noch kein umfassender Überblick darüber vorliegt, in welchen AKW in welchen Bereichen die Siemens-Software, auf die Stuxnet abzielt, eingesetzt wird, welche teilweisen Informationen liegen der GRS mbH bereits zu welchen AKW dazu vor (vgl. Seite 4 in der Weiterleitungsnachricht der GRS mbH)?

4. Wie schließt die Bundesregierung, für den Fall, dass auch deutsche AKW und weitere Industrieanlagen befallen sind, aus, dass es hierdurch zu schwerwiegenden Fehlern in den betrieblichen Abläufen kommt?

5. Wie bewertet die Bundesregierung, insbesondere hinsichtlich der Atomaufsicht, die Selbstauskunft der Siemens AG vom 11. März 2011, dass insgesamt weltweit 24 Kunden aus dem industriellen Umfeld von einer Stuxnet-Infektion berichtet haben und es in keinem Fall während einer Infektion zu Auswirkungen auf die Prozesssteuerung kam?

   Liegen der Bundesregierung hier differierende Einschätzungen vor, und wenn dies der Fall ist, wie lauten diese?

6. Ist der Bundesregierung, insbesondere dem BMU und Bundesamt für Sicherheit in der Informationstechnik (BSI), bekannt, welche anderen Länder mit AKW Analysen veranlasst haben, die mit der Weiterleitungsnachricht der GRS mbH vergleichbar sind?

   Falls ja, welche Staaten haben wann welche Untersuchungen veranlasst, und welche (Zwischen-)Ergebnisse liegen bereits vor?

7. Inwiefern ist die Sicherheitsrelevanz von Malware wie Stuxnet bereits Gegenstand der internationalen Zusammenarbeit des BMU zur Reaktorsicherheit?

   Inwiefern war sie es insbesondere auf der Fünften Überprüfungskonferenz zum Übereinkommen über nukleare Sicherheit im April 2011 in Wien?

8. Ist es korrekt, dass die Nachweise zur Störfallbeherrschung davon ausgehen, dass sich die Anlage in einem bestimmten, definierten Ausgangszustand befindet?

9. Kann praktisch ausgeschlossen werden, dass Malware wie Stuxnet Anlagekomponenten so schädigt, dass der tatsächliche Zustand bzw. das tatsächliche Verhalten bestimmter Komponenten nicht dem angezeigten bzw. übermittelten Zustand/Verhalten entspricht, und dies dann insbesondere mit bislang nicht berücksichtigten Implikationen für die Störfallbeherrschung verbunden ist?

   Falls ja, weshalb und auf welche wissenschaftliche Grundlage (Untersuchungen, Stellungnahmen, Gutachten etc.) stützt sich die Bundesregierung dabei?

10. Kann praktisch ausgeschlossen werden, dass Malware wie Stuxnet ein AKW unbemerkt aus den betrieblichen Begrenzungen herausführt, und dies dann insbesondere mit bislang nicht berücksichtigten Implikationen für die Störfallbeherrschung verbunden ist?

    Falls ja, weshalb und auf welche spezifische wissenschaftliche Grundlage (Untersuchungen, Stellungnahmen, Gutachten etc.) stützt sich die Bundesregierung dabei?

11. Welche BSI-Leitlinien, -Standards und Hilfedokumente sollen anlässlich des Aufkommens von Stuxnet bis wann überarbeitet werden?

    Sind dabei neue BSI-Leitlinien und -Standards geplant oder bereits erlassen, die speziell auf AKW zugeschnitten sind?

12. Auf welche Art und Weise wird die Bundesregierung die Empfehlung des BSI, industrielle Prozesssteuerungsanlagen vom Internet getrennt zu halten (Die Lage der IT-Sicherheit in Deutschland 2011, S. 29), bei AKW dauerhaft umsetzen?

13. Inwiefern ist Malware wie Stuxnet Gegenstand der Beratungen im sog. Cyberabwehrzentrum und dem sog. Cybersicherheitsrat, und wenn ja, wie werden die dort ausgetauschten Kenntnisse an Atomaufsichtsbehörden kommuniziert?

14. Welche Auswirkungen haben die durch Stuxnet gewonnenen Erkenntnisse auf die Pläne der Bundesregierung zum verbesserten Schutz kritischer Infrastrukturen, und welche zum Beispiel im „Dritten Gefahrenbericht“ der Schutzkommission beim Bundesministerium des Inneren angemahnt und teilweise in der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie) und im „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) umgesetzt wurden?

15. Ist die Bundesregierung, auch vor dem Hintergrund, dass es im NPSI heißt, dass es „um den Schutz der Informationsinfrastrukturen in Deutschland nachhaltig zu gewährleisten“ erforderlich sei, den Nationalen Plan und dessen Umsetzung regelmäßig anzupassen und ihn gegebenenfalls an die aktuellen Erfordernisse anzupassen, der Ansicht, dass der NPSI angesichts der anhand des Stuxnet-Befalls gewonnenen Erkenntnisse grundlegend überarbeitet werden muss?

    Wenn ja, welche Anpassungen werden hier vorgenommen?

    Wenn nein, warum soll keine Anpassung erfolgen?

16. Welche neuen IT-basierten Kontrollmechanismen sind speziell für deutsche AKW im Einsatz oder geplant, um einen Stuxnet-Befall feststellen zu können und andere gezielte Angriffe abzuwehren?

17. Gibt es grundsätzlich einheitliche Richtlinien für die IT-Sicherheit in AKW?

    Falls ja, seit wann, wann wurden sie zuletzt geändert und durch wen wird

    a) ihre Einhaltung und

    b) ihre Effektivität

    kontrolliert und

    c) jeweils wie regelmäßig?

    Welche Informationen hierzu liegen dem BMU und den Landesatomaufsichtsbehörden hierzu vor?

18. Falls es einheitliche verbindliche Richtlinien für die IT-Sicherheit in AKW gibt, wann gab es in welchen Anlagen welche Verstöße dagegen?

    Wie wurden sie geahndet?

19. Ist seitens der Atomaufsichtsbehörden geplant, anlässlich hochentwickelter Malware wie Stuxnet verbindliche neue IT-Sicherheitsvorschriften zu erlassen?

    Muss dafür aus Sicht der Bundesregierung gewartet werden, bis die Auswertung der aktuell laufenden Weiterleitungsnachricht der GRS mbH erfolgt ist (bitte begründen)?

20. Ist die Weiterleitungsnachricht der GRS mbH aus Sicht des BMU und des BSI geeignet und ausreichend, um praktisch auszuschließen, dass in AKW eingesetzte Rechner von Malware wie Stuxnet befallen werden (ggf. bitte mit ausführlicher Begründung)?

Falls nein, welche Konsequenzen

a) hat die Bundesregierung daraus bereits gezogen, und

b) will sie daraus bis wann noch ziehen?

21. Welchen Zeitplan gibt es seitens des BMU für den weiteren Umgang mit den Risiken für den AKW-Betrieb und die Reaktorsicherheit, die sich aus Malware wie Stuxnet ergeben (bitte auch mit Beschreibung etwaiger Zwischenschritte und inwiefern das BMU dabei mit BSI, GRS mbH, den Landesatomaufsichtsbehörden, Cyberabwehrzentrum, Cybersicherheitsrat und anderen kooperieren will)?

22. Können das BMU und/oder die GRS mbH bestätigen, dass die Weiterleitungsnachricht zu Stuxnet nur empfiehlt, im Fall einer Stuxnet-Infizierung einer Steuerungsanlage sofort eine Analyse durchzuführen, um festzustellen, welche Auswirkungen eine Fehlfunktion haben könnte, die durch den Befall ausgelöst werden könnte?

23. Warum wurde nicht empfohlen, grundsätzlich bei allen im Zusammenhang mit Stuxnet-relevanten AKW-Steuerungsanlagen zu analysieren, welche Auswirkungen eine Fehlfunktion haben könnte, die durch einen Stuxnet-Befall ausgelöst werden kann?

24. Ist dies noch beabsichtigt?

    Falls ja, bis wann?

    Falls nein, warum nicht?

Berlin, den 15. Juli 2011

Renate Künast, Jürgen Trittin und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333